UNIDIR

International Law and State Behaviour in Cyberspace Series

Africa Regional Seminar: Conference Report

UNIDIR RESOURCES

Acknowledgements

This meeting is the second in a series of regional meetings in the framework of the UNIDIR project "International Law and State Behaviour in Cyberspace". UNIDIR would like to thank the governments of Germany, the Netherlands and Switzerland for their financial support for this project.

In addition, UNIDIR would like to thank the government of the Republic of Kenya for supporting this regional meeting.

The report was drafted by Aicha Bachir.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR)—an autonomous institute within the United Nations—conducts research on disarmament and security. UNIDIR is based in Geneva, Switzerland, the centre for bilateral and multilateral disarmament and non-proliferation negotiations, and home of the Conference on Disarmament. The Institute explores current issues pertaining to the variety of existing and future armaments, as well as global diplomacy and local tensions and conflicts. Working with researchers, diplomats, government officials, NGOs and other institutions since 1980, UNIDIR acts as a bridge between the research community and governments. UNIDIR's activities are funded by contributions from governments and donor foundations.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The views expressed in this publication are the sole responsibility of UNIDIR. They do not necessarily reflect the views or opinions of the United Nations or UNIDIR's sponsors.

www.unidir.org

International Law and State Behaviour in Cyberspace Series

Africa Regional Seminar

Conference Report

3–4 March 2015, Nairobi, Republic of Kenya

Introduction

As part of its International Law and State Behaviour in Cyberspace Series, UNIDIR carried out its Africa Regional Seminar on 3–4 March 2015 in Nairobi, Republic of Kenya.

Over the past two decades, there has been a growing reliance on cyberspace applications across a broad spectrum of activities and processes. As governments and societies increasingly depend on cyberspace in their daily activities, there is an urgent need to determine how existing international legal instruments and norms apply in the borderless and fast-evolving world of cyberspace. Among governments and in academia, there is a consensus that international law does apply in cyberspace; however the question remains: in what ways does it apply? In light of the 2012–2013 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) report—which noted the applicability of international law—and the convening of the fourth GGE in 2014–2015, it is an opportune time to explore this question and related conversations.

In pursuit of this, the Africa Regional seminar brought together both legal and policy voices to explore the cyber domain's legal context as it relates to the African region. This meeting provided an opportunity for regional stakeholders to exchange views and opinions, and to engage in a dialogue on the complexities and various interpretations of the applicability of international law in cyberspace within national frameworks. The seminar aimed to promote greater regional understanding, as well as to provide participants with a network of contacts throughout the region that in the long term might allow for better communication and cooperation on cyber issues.

PROCEEDINGS

Conference Chair

- **Mr. Ben Baseley-Walker**, Programme Lead, Emerging Security Threats, UNIDIR

Welcoming Remarks

- **Ambassador Anthony Andanje**, Director, Multilateral Affairs, Ministry of Foreign Affairs, Republic of Kenya

Opening Remarks

- **Mr. Ben Baseley-Walker**, Programme Lead, Emerging Security Threats, UNIDIR

Ambassador Andanje opened the seminar by extending to all participants a warm welcome from the Republic of Kenya and thanking UNIDIR for bringing the region together to discuss the important topic of cyber and international law. He noted that cyber is a growing resource on which all states are increasingly dependent, and there is a growing reliance on cyberspace applications throughout government and private sector activities. In addition to the significant contribution of the cyber domain to socioeconomic development, this rapidly developing area poses enormous challenges and risks. Ambassador Andanje outlined that today cyber warfare occupies a central position in the military doctrine of some states, as demonstrated by the substantial spending and resource usage being applied to creating advanced offensive cyber capabilities. In order to address the many challenges posed by the cyber domain, all states and stakeholders have a role to play in working towards cyber stability, part of which requires addressing critical cyber issues such as attribution and state responsibility. There have been key developments on state behaviour in cyberspace at multilateral and regional levels and that, with both the United Nations General Assembly resolution 5370 and the GGE, there is recognition that international law applies to state behaviour in the use of ICT.

Ambassador Andanje explained that Kenya is involved in both regional and international cooperation on key issues in the cyber domain, including being an active participant in the GGE, as Kenya considers that the group is contributing to significant changes at the multilateral level. He added that although Africa is facing several challenges on the policy and security aspects of cyber issues, it is critical that, as new and growing stakeholders, African states should participate effectively in developing parameters for responsible activity in the cyber domain in order to maximize national benefits in the long term. The adoption of the African Union (AU) Convention on Cybersecurity and Personal Data Protection in June 2014 was seen as a positive development and is a testament to the efforts being made in the region to craft legal instruments on cyber. Finally, he affirmed that all African states have a clear interest as well as a clear responsibility to uphold international law and maintain international order.

In Mr. Baseley-Walker's opening remarks, he underlined that cyber is the game changer of our age and something all states have an interest in. As an issue that cuts across multiple other subject areas, it is a challenging one to address and regulate. Unlike traditional areas of policy and law, the difficulty with cyber lies in the fact that, for many new entrants, approaches to policy and other initiatives have to be developed on three different levels

simultaneously: national, regional and multilateral. Indeed, today states may resort to using traditional policy processes ill-adapted to cyber, which is a fast evolving area, requiring decisions to be made in short time frames.

He explained that UNIDIR's International Law and State Behaviour in Cyberspace Series seeks to engage a broad spectrum of stakeholders, including those who perhaps historically have not had a major voice in international security and dialogue on cyber, and to provide a space for their input in pragmatic dialogue on the development and the applicability of international law to the cyber domain. By providing a platform for a regional discussion on issues that African states are facing in the cyber domain, it is hoped that participants could explore how cyber may be a destabilizing component in ongoing international security relations and consider how to mitigate the risk that cyber becomes a trigger for instability and conflict in the future.

Panel 1. Introductory Context

- **Why Cyber Matters in Africa—Looking to the Future**
  Ms. Dorothy K. Gordon, Director-General, Ghana–India Kofi Annan Centre of Excellence in Information and Communication Technology
- **Cyber and Development in the African Region**
  Dr. Towela Nyirenda-Jere, Programme Manager, e-Africa Programme, The New Partnership for Africa's Development Planning and Coordinating Agency
- **Obligations, Rights and Responsibilities in Cyberspace**
  Mr. Michael Katundu, Director of Information Technology, Communications Regulatory Authority, Communications Commission of Kenya, Republic of Kenya

A key aim for this seminar was to encourage an exploration of the issues most relevant to African states and to allow regional perspectives and differences to be discussed, thereby increasing understanding among neighbouring states. It sought to link the cyber conversation with the international policy climate, helping highlight the far-reaching impacts of cyber insecurity or instability in other realms of international relations. Panel 1 laid out the foundations for such discussions by expanding on the importance of cyberspace to both the African region's development and the international policy context.

Ms. Gordon presented on the importance of cyber in Africa and the steps that the continent must take for the future. She began by noting that cyber engagement is a question of survival for Africa and that states need to coordinate on this issue in order to develop ICT capabilities and adequate cyberspace regulation. She considers that cyber increasingly matters to Africa because African economies are becoming more integrated with the global economy, and cyber issues arising in one country can easily spread to others. As technological innovation spreads across the African region and more citizens gain access to the cyber domain, governments are exploring legal ways to best use and secure cyber technologies. However, dealing with the use of new technologies to provide services to citizens has put a tremendous stress on already stressed governments. The task of managing and protecting private data has become increasingly challenging—both for governments in terms of the rights and privacy of users, and for law enforcement agencies in conducting investigations. She noted that addressing the realms of the Internet where criminals reside is a global issue and governments must be aware of the risks and crimes posed by new technologies in order to create appropriate international and national legal instruments.

To address these new types of challenges that the continent is facing, Ms. Gordon laid out several recommendations: creation of a regional information-sharing mechanism on threats and risk mitigation; use of transparent security systems for critical national infrastructures; education of the public/private sector and governments on cyberspace; cooperation with the private sector; participation in global decision-making processes, and the development of national policies on cyber. Finally, she underlined the necessity of adapting, at a regional level, the multi-stakeholder models used at the international level.

Dr. Nyirenda-Jere then explored the relationship between cyber and development in the African region. The New Partnership for Africa's Development (NEPAD) has been conducting several projects to create capacity in the areas of cyber stability and security to enable states to address the issues and challenges brought by the use of this technology. She illustrated her presentation with an overview of NEPAD's strategic work in cyber within its e-Africa programme, which has a number of focus areas for ICT, including broadband infrastructures, capacity development, creating an enabling environment and e-applications and services.

One facet of NEPAD's efforts is improving terrestrial Internet connectivity between all capitals in the region, as at present most Internet data is routed via Europe. However, in connecting the capitals together, cross-border infrastructures and services present challenges in terms of regulation. To address this challenge, NEPAD, in coordination with the AU, has developed national Internet Exchange Points (IXPs), and the AU is encouraging the creation of subregional Internet exchange points to provide another level of aggregation. The IXPs will allow for local economies to have their traffic routed and managed locally by Internet service providers through their local infrastructures instead of routing traffic via locations outside the continent.

Dr. Nyirenda-Jere underlined that NEPAD also works to encourage a multi-stakeholder approach to Internet governance, and considers capacity-building to be a key element in dealing with cyber issues globally. In 2013, NEPAD created the African School on Internet Governance to address the education gap; however, it was noted that capacity-building in national higher education systems in Africa is still missing. In summation, Dr. Nyirenda-Jere encouraged states to work with a multi-stakeholder or multisectoral approach, and to trust the various stakeholder groupings in the area.

Mr. Katundu's presentation addressed the issues related to obligations, rights and responsibilities in cyberspace. He started his presentation by referring to the World Summit on the Information Society (WSIS) of 2003 and 2005 organized by the International Telecommunication Union (ITU), where states recognized that "all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the Internet". He explained that Kenya has developed a number of policies, strategies, institutions and frameworks towards these goals. He indicated that within the current "Vision 2030" strategy for development that Kenya is implementing, ICT does not constitute one of the three pillars; however, it is part of every pillar—and the Vision's objectives cannot be achieved without ICT. He indicated that Kenya has also created an ICT regulatory authority and a national Computer Incident Response Team (CIRT), both of which are playing key roles in the development and implementation of policies, laws and regulations for cyber security.

Mr. Katundu outlined that in developing relevant policies and legal instruments for the promotion and use of a safe cyberspace, governments must consider the obligations, rights and the responsibilities of citizens. When using ICT, citizens must remain protected, and

therefore governments must develop national policies and educate citizens on these rights and responsibilities. Governments must also implement laws and regulations in accordance with international law on new areas such as e-transactions, consumer protection, data and privacy protection, and cybercrime—in order to address the challenges these new areas pose to citizens.

In addition to the legal and policy framework, Mr. Katundu stressed that governments must ensure that various technical and policy aspects are addressed, including identification and protection of national critical information infrastructure; progress towards local, regional and international cooperation and collaboration on cybersecurity incidents; the development of international standards and legal principles on cybersecurity and related technologies; a coordinated technology watch and early warning network; capacity-building across all areas dealing with ICT; and the creation of consumer awareness in the use of new technologies. Finally, Mr. Katundu noted that achieving a safe and secure cyberspace is a collaborative effort and all cyber stakeholders have a role to play.

The discussion period raised questions on the challenges associated with coordination between intelligence and security agencies, and the necessity of capacity-building. In the area of intelligence and security, one participant suggested that all public and private cyber stakeholders should be brought together to coordinate with each other. Another participant noted that there is no best practice yet when it comes to guarding against infringement of citizens' rights with respect to their data, and that without regulation, this situation can lead to abuse. On capacity-building, one participant emphasized that this must be implemented in every sector of a society, with specific needs identified in order that any training or strategy developed can address needs in a targeted way. Another participant noted that education in ICT and cybersecurity was a key component for capacity-building in cyberspace and that states should start educating and training their citizens to develop capabilities and expertise.

Panel 2. The Legal Landscape

- **International Law and Cyber 101: An Introduction**
  Ms. Angela Ng'ang'a, Corporate Affairs Lead ESA and IOI, Legal and Corporate Affairs, Middle East and Africa, Microsoft Corporation
- **Current Mechanisms for Addressing Cyber at the Africa Regional Level**
  Ms. Amazouz Souhila, Senior Radio Transmission and Broadcasting Office, Infrastructure and Energy Department, African Union Commission
- **Regime Coherence: National, Regional and Multilateral Legal Interaction on Cyber Issues**
  Mr. Preetam Maloor, Strategy and Policy Advisor, International Telecommunication Union

Panel 2 tackled some of the major topics and questions raised by legal experts and states in the application of international law to the fast-moving and borderless cyber environment. From the private sector to governments, the issue of cyber requires the re-examination of the definitions of national and international principles, and the implementation of legal frameworks and mechanisms at the national, regional and international levels to regulate the challenges encountered in cyberspace.

Ms. Ng'ang'a opened the panel with a presentation on the basics of international law and cyber, and given her particular expertise, provided participants with information on how Microsoft regards legal obligations and consumers rights. Microsoft has been tackling the specific issues of cybercrime and cybersecurity a great deal, including establishing a digital crimes unit to explore how they can support customers and governments with understanding how to deal with the various new trends in technology.

Ms. Ng'ang'a noted that as the pace of activity in cyber increases, so does the likelihood of governments misinterpreting the actions of one another, and the risk of a cyber war cannot be discounted. She outlined that as cyber threats continue to grow, governments are looking at the ways in which they can protect their citizens. This tends to increase the need for access to data for law enforcement and intelligence matters, however governments may also exploit networks for a number of other reasons including economic espionage, military espionage and operations. Considering this, Microsoft has found that an increasing number of states are developing both defensive and offensive cybersecurity capabilities to prevent and fight back against cyber attacks.

Against this backdrop, Microsoft promotes the establishment of international cybersecurity norms to limit the potential of conflict in cyberspace and to define what state behaviour in cyberspace should be with regard to international law, so that events do not escalate to warfare. Ms. Ng'ang'a shared with the panel several norms that Microsoft promotes: states should not target ICT companies to insert vulnerabilities, or take actions that would undermine public trust in products and services; states should have a clear policy for handling privacy issues and security vulnerabilities with a mandate to report to vendors rather than to stockpile or exploit them; states should exercise restraint in developing cyberweapons and should ensure that any that are developed are limited, precise, and not reusable consistent with the concept of "distinction, discrimination and distribution" to limit the impact associated with these actions; states should commit to non-proliferation activities related to cyberweapons; and finally, that states should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.

Next, Ms. Amazouz explored the current mechanisms for addressing cyber at the African regional level. She noted that while African countries' access to broadband and Internet has increased, issues related to cybersecurity and cybercrime are still emerging. In many countries there is a lack of know-how in terms of cybersecurity and an inability to monitor and protect local networks, making African countries particularly vulnerable to incidents of cyberterrorism and cyberespionage. She suggested that for some states there is an inability to develop the legal frameworks to fight cybercrime, and for others, the level of implementation of legislation and deployment of security systems in the private and public sectors is low.

The presentation then showcased the work of the AU, which encourages states to cooperate and to combat cybercrime through a multi-stakeholder approach, involving both governments and industries. She added that considering the international dimension of cyber security, it is important to reinforce international cooperation on this issue particularly with regard to confidence-building measures (CBMs). To this effect, the AU has adopted a convention to address the cyber issue and to mitigate the risks deriving from misuse of ICTs. The objective is to define a regional harmonized framework for cybersecurity legislation, to develop general principles as specific provisions related to cyber legislation, to outline cyber legislation measures required at the member state level, and to develop general or specific provisions on international cooperation related to cyber legislation. The convention

embodies all aspects of cyberspace, including organization of e-commerce, the protection of personal data, the promotion of cybersecurity, and the fight against cybercrime. In this latter regard, the criminal provisions of the convention specifically set out definitions of ICT offences and adapt certain sanctions for ICT offences.

Ms. Amazouz stressed that the AU is also focused on assisting states in setting up their national legislation. By adopting the AU convention and transposing it into national policies, the different model laws and guidelines implemented by states will allow for the development of a more harmonized regional legal framework built on minimum common standards, principles and procedures in the regulation of cyberspace and the fight against cybercrime.

Mr. Maloor's presentation then focused on national, regional and multilateral interactions on cyber issues. Mr. Maloor outlined that facilitating the formulation of national strategies is key to creating effective measures for cybersecurity and stability. In this regard, the ITU works with ICT ministries to help set up ground infrastructures and basic capacity levels. Believing that capacity-building is a central foundation for cyber stability and security, the ITU provides states with technical assistance on mitigating risks, identifying best practices in legislation, and information-sharing. One initiative the ITU has launched is a subregional programme called "Support for Harmonization of the ICT Policies in Sub-Saharan Africa" (HIPSSA) to provide states with adapted responses for cyber incidents and to establish harmonized policy along with legal and regulatory frameworks at the regional and continental levels. The goal of this programme is to create an enabling environment that will attract investment, to foster the sustainable development of competitive African ICT regional markets and infrastructures, and to increase access of its people to related services.

In addition to these flagship projects, the ITU also provides in-country technical assistance for transposing international and regional guidelines to accommodate national specificities; has produced a guide to understanding cybercrime; carries out capacity-building under the coordination of the World Bank; and provides national assessment as well as public–private cooperation through national CIRTs. With regard to cooperation, Mr. Maloor emphasized that to have a global, effective level of cybersecurity, a coordinated, multilevel approach is needed. While Africa is doing well at the international and regional levels, it requires assistance in the implementation of relevant measures at the national level.

The discussions from this panel centred on the legal issues of privacy and vulnerability in the use of ICTs, and on the work of the AU to ensure the development of global legal norms and provisions. One participant enquired about the legal obligations of companies to provide secure technologies to governments and citizens. Another responded that privacy is critical, and that companies such as Microsoft work to ensure the integrity and reliability of their data and systems as they are entrusted by customers to hold their data. On the role of the AU to create global legal norms, one participant asserted that the AU believes cybersecurity is a global matter and thus should be managed in a global and integrated way. Accordingly, it was noted that the AU convention calls for all African states to be part of the process by setting up their national strategies in a way that involves all stakeholders and civil society.

Keynote Speech

- **African Imperatives in Cyber Norm Development**
  Dr. Katherine Getao, Information and Communications Technology Secretary, Ministry of Information and Communications Technology, Republic of Kenya

Dr. Getao's keynote presentation centred on African imperatives in cyber norm development, and outlined the importance of establishing cyber norms. She noted that as states are increasingly asked to take responsibility for certain aspects of cyberspace, it is necessary to define their sphere of responsibility. Even though the GGE affirmed that national laws apply to cyberspace, the interpretation and the application of laws remains an ongoing issue. She stressed that cyberspace and security are important items on national agendas, and cooperation among states will enhance regional and international agendas.

Looking briefly at the East African regional cyber landscape, she explained that there are some regional bodies and processes already in place, and that states recognize the importance of CIRTs as well as the importance of national strategy and implementation plans on cyber issues. She remarked that in this subregion national processes on cyberspace and cybersecurity are much more supported, advanced and robust than regional and international processes, as the multi-stakeholder approach requires time for institutions to learn to work together. Furthermore, there were seen to be multiple regional organizations working on cyber issues in East Africa, and each and every state is part of one or more of them, which adds complexity to harmonization and implementation. She suggested that, more broadly, cyber norms could be developed through the framework proposed by the AU convention, which calls for a definition of the role of governments, the development of policies and plans, provision of a broad legal framework for drafting national legislations, the identification of relevant authorities and institutions, and the outlining of important principles for cyberspace.

As a way to move forward, Dr. Getao laid out several recommendations: the creation of awareness- and capacity-building programmes; the implementation of a cyber norm agenda from the AU convention within national governments; and the possible creation of an AU Group of Governmental Experts in regional security and diplomacy in cyberspace. This latter proposal was largely supported by participants during the floor discussion.

Panel 3. Cyber Concepts

- **Attribution in Cyber: Responsibility for State and Non-State Activities**
  Ms. Jemima Njeri, Senior Researcher, International Crime in Africa Programme, Transnational Threats and International Crime Division, Institute for Security Studies Africa
- **Improving Cyber Access: Possible Threats and Challenges**
  Mr. Kodzo Gadzekpo (Marcus) Adomey, Education and Research Manager, AfricaCERT
- **Chain Reactions: Understanding Knock-on Effects in Cyberspace**
  Mr. Jonathan Ledgard, Director, Afrotech, École Polytechnique Fédérale de Lausanne

Panel 3 examined the basis for some of the legal and political concepts frequently employed in international forums and processes relating to the cyber domain. Some of the most discussed key concepts are attribution and responsibility in the cyberspace environment.

Exploring the issues encountered with these concepts when viewed in the context of cyber activity is an essential step to addressing the main challenges and ultimately to applying these terms to the cyber environment.

Ms. Njeri focused her presentation on attribution in cyberspace, specifically looking at responsibilities for state and non-state activities. She began by saying that in the context of international law, attribution is an essential and indispensable action, yet attributing certain cyber attacks to a specific actor can be difficult, or in the case of well-funded militaries, impossible, as the identity of perpetrators can be easily disguised and the origination point of the attack hidden. She noted that following a cyber attack accusations may be addressed without sufficient technical evidence or basis, which, in the case of state actors, may lead to a loss of mutual trust detrimental to international relations.

Ms. Njeri explained that the complex challenges associated with cyber attacks include problems perceiving an attack's seriousness and motive, justifying appropriate responses, and identifying the appropriate legal frameworks that may apply. She considered that there are several factors that complicate the task of attribution in cyberspace. Firstly, cyberspace is a domain for both state and non-state actors, and they may carry out activities of diverse sophistication for a variety of purposes. Secondly, many cyber tools can be used for either legitimate or illegitimate purposes. Thirdly, the private sector is an increasingly major player in the domain, both involved in Internet controls as well as providing the systems and private platforms upon which states rely. Fourthly, there is no common understanding on applicable international rules and standards for state behaviour in the cyber domain.

Ms. Njeri underlined that depending on whether an attacker is a state, non-state or proxy actor, various aspects of international law may be applicable. In this regard, it is necessary to evaluate the role of international regulation, and to identify the technical and regulatory problems of attribution, as well as to explore possible solutions to cyber attacks when attribution cannot be achieved. She saw the absence of an international legal regime for cyberspace as a great challenge in terms of dealing with issues of attribution, and expressed that there is a necessity for not only an international legal framework, but also regional and national ones.

Mr. Adomey's presentation explored the possible threats and challenges to improving cyber access. He defined such threats and challenges as cyber "determinants" and identified three types of determinants:

- **Technological determinants** that are relevant to an organization to improve cyber access.
- **Organizational determinants** that are the characteristics and resources of an organization.
- **Environmental determinants** defined by the structure, the regulation and the level of technology service providers of an organization.

Although he sees a high level of politicization of cybersecurity issues, Mr. Adomey noted that it remains a low priority area in most states, as evidenced by the porosity of laws and the slow speed of processes establishing them. In order to address these challenges, he recommended that states enact measures to increase national awareness, to promote the development of technical skills in the region, to build strong and depoliticized cybersecurity institutions, to participate in a regional security strategy, and to create effective computer

emergency response teams (CERTs). Finally, he proposed that states should consult, collaborate and cooperate with each other, with trust, to ensure overall cybersecurity.

Mr. Ledgard closed out the panel by sharing his perspectives on the possible future of African countries with regard to the development of Internet technology and high connectivity. He suggested that in the future a generation of Africans with low incomes but a high degree of Internet connectivity could generate large political dissonance across the continent. He felt that a lot of work in the region is still needed to ensure the security and safety of the cyber domain, especially considering that in future it will not only be a major space for communication but for commerce as well. As an example, Mr. Ledgard explained that the development of new technology such as cargo drones could allow the movement of goods more efficiently, effectively, and economically across the continent, which would be a revolutionary option for African economies. However, he noted that using cargo drones requires a high degree of connectivity that could expose the system to vulnerabilities.

The discussion session of this panel focused largely on the issue of attribution. One participant asked if there was any possibility of finding a methodology such as the one used in the traditional legal domain to enable prosecution even if complete certainty of guilt or innocence cannot be secured, and to consider the implications of punishing those that failed to protect when obligated. Another participant responded that, unfortunately, attribution is so broad that it can entail issues with political implications, therefore certainty appears to be mandatory, and thus called for policies, standards and guidelines to obtain and ensure this certainty. It was also raised that the problem of attribution is a technical one in terms of the available tools to trace the origins of a cybercrime that involve some illegal use of technology.

Panel 4. Cyber Stability

- **Cyber Conflict and International Law**
  Dr. Nils Melzer, Senior Advisor, Security Policy Division, Political Directorate, Swiss Federal Department of Foreign Affairs, Swiss Confederation
- **An Arab African Perspective on Multilateral Approaches to Cyber Conflict and Cybersecurity**
  Mr. Amr Aljowaily, Minister Plenipotentiary, Permanent Mission of Egypt to the United Nations in New York, Arab Republic of Egypt
- **The Role of Cyber in International Peace and Security**
  Dr. Eneken Tikk-Ringas, Senior Fellow for Cybersecurity, International Institute for Strategic Studies: Middle East Office

Panel 4 explored a major issue in many national and multilateral discussions on security in cyberspace—stability. Panellists explored the legal underpinnings of the use of force in cyberspace and defining cybersecurity under international law, as well as the ways in which cyber warfare can be understood in both the United Nations and international humanitarian law context.

Mr. Meltzer's presentation explored international law instruments applicable to cyber conflict. He identified several bodies of law that are applicable in the area of cyberspace, among which are the Charter of the United Nations which prohibits the use of force in international relations, international humanitarian law in armed conflict, and the obligations and rights of neutral states in conflict. Mr. Meltzer underlined the significance of the definition of the

use force in cyberspace for states, as they can only resort to self-defence if force is used against them in the sense of the Charter. However, if this threshold is not met, states can still use countermeasures that are below the generally-agreed United Nations threshold of the use of force. He added that if use of force is actually perceived in cyberspace by a state, the law of conflict would be applicable.

With regard to international humanitarian law, Mr. Meltzer asserted that a distinction must be made between civilian and military persons and objects, and explained that an attack is defined as an "act of violence in offence or defence". In this context, it could therefore be argued that states cannot legally attack civilian data and infrastructures in cyberspace. He noted that while there are difficulties in literally applying the existing treaties, there is common agreement that international humanitarian law can apply to cyberspace, however the difficulties lie in identifying the underlying legal principles.

Mr. Aljowaily presented an overview of multilateral approaches to ICTs and international peace and security. He started by emphasizing that it is important to understand that states conceptualize their international security policy according to different security paradigms and perspectives. Some states, for example, use three points of departure when addressing a cybersecurity issue: national security, homeland security and human security; and when analysing their national interests, states rely on the perception or evaluation of the magnitude of threats in the determination of policy.

Within the United Nations framework, he added, there exist three different perspectives for dealing with international security issues and international peace and security issues in general:

- regulation/arms control versus disarmament perspectives;
- trust and confidence-building measures versus prevention of an arms race; and
- pacific settlement of disputes

Mr. Aljowaily underlined that the threshold of definition for the use of force in cyberspace is not very high, considering that developing countries that have a lack of resources to address cybersecurity challenges posed by new technologies are far more vulnerable than developed countries to any form of disruption that may happen. He explained that in the context of ICT security the threat or use of force would also encompass the destruction or harm, in any form, of any of the three interlinked layers of the Internet, namely telecommunications and related infrastructure; technical standards; and content and its related applications. He considered that any form of deliberate disruption of one of these three layers can amount to a use of force, and thus fall under article 2 (4) of the Charter of the United Nations.

Finally, Mr. Aljowaily endorsed regular institutional dialogue on ICT security issues with broad participation under the auspices of the United Nations, as recommended by the GGE; and with regards to attribution, he underlined that all states must participate in all arrangements related to the management and governance of critical Internet infrastructure and Internet governance mechanisms.

Ms. Tikk-Ringas then discussed the role of cyber in international peace and security. She saw cybersecurity as broad and composed of technical as well as non-technical aspects which, in her opinion, explain why international cybersecurity consists of a number of questions that simultaneously involve many areas. She asserted that from a national perspective there are different priorities, capabilities and issues which every government should identify so that

the international community can understand how they can be comprehensively addressed to fit into regional conversations, consensus, and potentially, common international understanding and principles. She also encouraged the international community to embrace inclusive dialogue that would encompass governments alongside individuals, associations, enterprises and other organizations active in the private sector.

Ms. Tikk-Ringas remarked that we have entered a period in which it has become normal for states to develop military cyber capabilities, and that today cyber might be used in armed conflict or to pursue political goals. In such a context, she believes the international community can rely on several types of binding and non-binding international legal instruments to regulate and secure cyberspace. While there are 250 existing instruments adopted by different international organizations on the issue of cybersecurity, Ms. Tikk-Ringas encouraged states to think about how to resolve issues nationally or regionally, and to adapt international norms to specific contexts. She cautioned that everything could not always be decided at the international level, but that any chosen decisions should always be guided by law.

The discussion session explored the principle of territorial sovereignty in cyberspace, the perception of threats and the relevance of the Geneva Conventions to cyber activities. One participant asked if national territorial integrity applies to cyberspace and how one might define cyber attacks or incidents in terms of a threat to a state's security. One participant responded that in terms of sovereignty states are bound to existing principles, therefore the real question lies in how states interpret the concept of sovereignty. Another participant noted that within the three layers of the Internet, sovereignty applies predominantly to telecommunication infrastructures. With regard to the magnitude of threats, the participant considered that the lower the threshold is, the more developing countries are protected. Finally, one participant explained that the original Geneva Conventions were drafted to regulate relations and conflicts between states, however nowadays, actors in armed conflicts are no longer only states. Thus, it was suggested that international humanitarian law must evolve in its normative content and in its application of norms and principles to new technology.

Panel 5. Cyber and International Peace and Security: National Approaches to Legal Development

- **Republic of Cameroon**
  Ms. Balbine Manga, Attorney and Information and Communication Technology Consultant, Organisation Internationale de la Francophonie
- **Republic of Rwanda**
  Ms. Florida Kabasinga, Senior Legal Advisor, International Crimes Department, National Public Prosecution Authority, Republic of Rwanda

The final panel explored various national developments and perspectives on the international peace and security aspects of cyber issues. In driving the international law and cybersecurity conversation forward and building consensus on key issues, it is important to express national approaches and understandings on existing international law.

Commencing this panel, Ms. Manga presented the Cameroonian national perspective on law in cyberspace. She remarked that the geographical localization of the country in central Africa makes it an interesting example, as it shares boundaries with more than five countries.

She explained that cyber is one of the problems shared across borders in the subregion, while mobile connectivity and the high use of social media also bring new threats to the country.

She mentioned that Cameroon has implemented national institutions in charge of cybersecurity and the national legal framework is inspired by the Economic Commission for Africa (ECAS) regional framework. The laws encompass issues related to the use of ICTs, to cybersecurity and criminality. However, Ms. Manga recognized that all these actions have yet to be implemented, and Cameroon, as in the case of many other countries, does not have sufficient capabilities to do so. Ms. Manga summed up that all institutions, at the national and regional levels, should work together in sharing practices, implementing laws and building capacities.

Speaking on the perspective of Rwanda, Ms. Kabasinga stated that cyberspace is regarded as an essential component for Rwandan economic development and its future. ICT penetration is very high in Rwanda and almost everything is available online. Ms. Manga noted that throughout all sectors there is a gap in awareness of what cybercrimes are and the endless possibilities of them, and yet at the same time the latest developments in technology are still embraced.

To tackle the challenges posed by cyberspace, Rwanda has created a legal framework that includes laws related to cybercrime. At the organizational level, the state has created specialized institutions and is trying to undertake capacity-building in all institutions dealing with cybercrime prosecution.

The final panel discussion revolved around the difficulties encountered in investigation and prosecution of transborder cybercrime. When not dealt with at the political level, the processes of investigation and prosecution rarely proceed, due to the lack of international mutual legal assistance for extradition on one hand, and the costs and benefits of dealing with the cases compared to the damages they create on the other hand. Unless a particular case involves high-impact crimes, most cases are rarely fully prosecuted, and often the victims are the first ones to give up on pursuing legal resolution.

Scenarios

The final session divided participants into groups and provided them with a hypothetical scenario involving transborder, malicious cyber activity. There was resounding agreement that in these emergency situations it was important to conduct forensic inquiries to identify the critical infrastructures that attacks were coming from through national CIRTs or regional organizations. Diplomacy and mediation were favoured as appropriate national approaches to the issue, and requests for extraditions were encouraged to prosecute the responsible individuals. One group focused on establishing cooperation with neighbouring states and regional organizations to identify the nature of the incident, and to ascertain if other states might have been victims as well. It was noted that if the problem appeared to be between states, it would be a political problem that needed to be dealt with diplomatically; if not, existing national institutions might be best suited to handle the matter. Another group discussed the crisis management response at the national level and the necessity for governments to publicly demonstrate their efficiency in containing the situation. The group proposed the possibility of establishing national tribunals dealing with specific cybercrime issues.

The discussion period showcased various interpretations, understandings, and approaches that participants took in managing and responding to malicious cyber activity. The discussion also highlighted the need for cooperation to extradite cybercriminals when they are not state-aligned. Overall, participants emphasized the use of diplomacy and other countermeasures that do not include force as the favoured primary national approaches.

Closing Remarks

The most common message heard throughout the seminar was the need for international cooperation and mutual legal assistance in the cyber domain. The general sentiment found among participants as regards international law and its application in cyberspace seemed to be that the international community needs to create norms and guidelines which governments can rely on in order to apply the concept and principles of international law within their national context. There is, therefore, a very long way to go in this conversation, but seminars and regional conferences such as this are a positive step in building consensus and enhancing cooperation in new difficult areas.

UNIDIR

International Law and State Behaviour in Cyberspace Series

Africa Regional Seminar
Conference Report

3–4 March 2015, Nairobi, Republic of Kenya

On 3–4 March 2015, the United Nations Institute for Disarmament Research (UNIDIR) carried out the Africa Regional Seminar as part of its International Law and State Behaviour in Cyberspace Series. Held in Nairobi, Republic of Kenya, the Seminar brought together a wide range of government and academic representatives from across the region to discuss some of the key components of international law and its application in the cyber domain.